

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC808 U.S. PTO
09/619699
07/19/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 1月25日

出 願 番 号

Application Number:

特願2000-016020

出 願 人

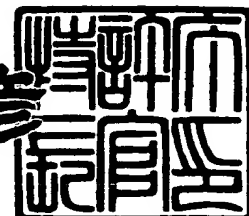
Applicant(s):

日本電信電話株式会社

2000年 6月23日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3046837

【書類名】 特許願

【整理番号】 NTTH116691

【提出日】 平成12年 1月25日

【あて先】 特許庁長官殿

【国際特許分類】 G06F

【発明者】

 【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

 【氏名】 森田 光

【発明者】

 【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

 【氏名】 小林 邦生

【特許出願人】

 【識別番号】 000004226

 【氏名又は名称】 日本電信電話株式会社

【代理人】

 【識別番号】 100066153

 【弁理士】

 【氏名又は名称】 草野 卓

【選任した代理人】

 【識別番号】 100100642

 【弁理士】

 【氏名又は名称】 稲垣 稔

【手数料の表示】

 【予納台帳番号】 002897

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9806848

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 大小比較装置・方法およびそのプログラム記録媒体

【特許請求の範囲】

【請求項 1】 1, 2, 3, ..., N の N 種の指標値に対し、初期値 IV に一方向性関数 h を多重（ここで、 IV に i 回の一方向性関数を施す場合、 $h^i(IV)$ と表現し、これは $h(h(h(\dots h(IV)\dots)))$ を意味し、 h 関数を i 回施すことを意味する。）に施した、 $h(IV)$, $h^2(IV)$, $h^3(IV)$, ..., $h^N(IV)$ なる値をそれぞれ対応させ、

複数人の参加者 J ($J = 1, 2, \dots$) が、それぞれ、 $(h^{N+1}(IV_J), g(h^i_J(IV_J)))$ (g は一方向性関数を示す) なる一対の値を示すことで、意中の指標値 i_J を間接的に登録し、

指標値 $N, N-1, N-2, \dots$ に登録した参加者 J がいるかどうかを指標値の大きい順に各指標値ごとに全参加者に問合せ手段により尋ね、該当しないときは、聞かれた指標値 m に対して各人 J が $h^m(IV_J)$ を答えることでその回答が $h^{N+1}(IV_J)$ から連なることを示し、ある参加者 K の指標値 i_K が聞かれた指標値 m に該当するときになって初めて、 $h^{i_K}(IV_K)$ を示す事が登録されていた $g(h^{i_K}(IV_K))$ に対応することで、 N 種の指標値における最大値を予め登録していた者であることを証明する大小比較装置において、

前記 1, 2, 3, ..., N の N 種の指標値に対し、 $P_1, P_2, P_3, \dots, P_N$ なる値がその大小順に対応付けられている換算テーブルが設けられ、かつ参加者に公開され、 $P_1, P_2, P_3, \dots, P_N$ なる値に対して登録された最大値又は最小値を求めることを特徴とする大小比較装置。

【請求項 2】 前記変換テーブルは前記 $P_1, P_2, P_3, \dots, P_N$ には $P_1 < P_2 < P_3 < \dots < P_N$ なる大小関係があり、かつある特定の上位桁以上の値のみを示し、

各参加者 J が間接的に登録したい値が、その上位桁の値と該当する指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J との和 $P_{i_J} + Q_J$ で表現されるとき、

前記一対の値 $(h^{N+1}(IV_J), g(h^i_J(IV_J)))$ に Q_J を加え、 $(h^{N+1}(IV_J), g(h^i_J(IV_J)), Q_J)$ を登録し、

前記問合せ手段は各指標値 $N, N-1, N-2, \dots$ ごとに、全参加者の Q_J における大きいものから順次尋ねる手段であることを特徴とする請求項1記載の大小比較装置。

【請求項3】 前記変換テーブルは前記 $P_1, P_2, P_3, \dots, P_N$ には $P_1 > P_2 > P_3 > \dots > P_N$ なる大小関係があり、かつある特定の上位桁以上の値のみを示し、

各参加者 J が間接的に登録したい値が、その上位桁の値と該当する指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J との和 $P_{i_J} + Q_J$ で表現されるとき、

前記一对の値 $(h^{N+1}(IV_J), g(h^{i_J}(IV_J)))$ に Q_J を加え、 $(h^{N+1}(IV_J), g(h^{i_J}(IV_J), Q_J))$ を登録し、

前記問合せ手段は各指標値 $N, N-1, N-2, \dots$ ごとに全参加者の Q_J における小さいものから順次尋ねる手段であることを特徴とする請求項1記載の大小比較装置。

【請求項4】 $1, 2, 3, \dots, N$ の N 種の指標値に対し、初期値 IV に一方方向性関数 h を多重に施して、 $H_1 = h(IV) \parallel f_1, H_2 = h(H_1) \parallel f_2, H_3 = h(H_2) \parallel f_3, \dots, H_N = h(H_{N-1}) \parallel f_N$ なる値をそれぞれ対応させ、フラグ $f_1 \sim f_N$ は意中の指標値 i の時の f_i とそれ以外の時のフラグとを異なる値として区別し、 $x \parallel y$ は x に y を連結することを示し、

複数人の参加者 J が、それぞれ、その意中の指標値 i_J のフラグ f_{i_J} を用いた $h(H_N)$ なる値を示すことで、意中の指標値 i_J を間接的に登録し、

指標値 $N, N-1, N-2, \dots$ に登録した参加者 J がいるかどうかを指標値の大きい順に各指標値ごとに全参加者に問合せ手段により尋ね、該当しないときは、聞かれた指標値 m に対して $H_m = h(H_{m-1}) \parallel f_m$ に相当する値を各人が答えることでその回答が $h(H_N)$ から連なることを示すとともに f_m により意中の値でないことを示し、ある参加者 K の指標値 i_K が聞かれた指標値 m に該当するときになって初めて、 $H_{i_K} = h(H_{i_K-1}) \parallel f_{i_K}$ を示し f_{i_K} が意中の値にあることを示すことで、 N 種の指標値における最大値を予め登録していた者であることを証明する大小比較装置において、

前記、 $1, 2, 3, \dots, N$ の N 種の指標値に対し、 P_1, P_2, P_3, \dots, P

N なる値がその大小順に対応付けられている換算テーブルが設けられ、かつ参加者に公開され、 $P_1, P_2, P_3, \dots, P_N$ なる値に対して登録された最大値又は最小値を求めることを特徴とする大小比較装置。

【請求項5】 前記変換テーブルは前記 $P_1, P_2, P_3, \dots, P_N$ なる値には $P_1 < P_2 < P_3 < \dots < P_N$ なる大小関係があり、かつ上位桁以上の値のみを示し、

各参加者 J が間接的に登録したい値が、その上位桁の値と該当する指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J との和 $P_{i_J} + Q_J$ で表現されるとき、

前記 $H_{(N+1)J} = h(H_{NJ})$ に Q_J を加え、 $(H_{(N+1)J}, Q_J)$ を登録し、

前記問合せ手段は、指標値 $N, N-1, N-2, \dots$ ごとに全参加者の Q_J における大きいものから順次尋ねる手段であることを特徴とする請求項4記載の大小比較装置。

【請求項6】 前記変換テーブルは前記 $P_1, P_2, P_3, \dots, P_N$ なる値には $P_1 > P_2 > P_3 > \dots > P_N$ なる大小関係があり、かつ上位桁以上の値のみを示し、

各参加者 J が間接的に登録したい値が、その上位桁の値と該当する指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J との和 $P_{i_J} + Q_J$ で表現されるとき、

前記 $H_{(N+1)J} = h(H_{NJ})$ に Q_J を加え、 $(H_{(N+1)J}, Q_J)$ を登録し、

前記問合せ手段は指標値 $N, N-1, N-2, \dots$ ごとに全参加者の Q_J における小さいものから順次尋ねる手段であることを特徴とする請求項4記載の大小比較装置。

【請求項7】 $1, 2, 3, \dots, N$ の N 種の指標値に対応して、初期値 IV に一方向性関数 h を多重（ここで、 IV に i 回の一方向性関数を施す場合、 $h^i(IV)$ と表現し、これは $h(h(h(\dots h(IV) \dots)))$ を意味し、 h 関数を i 回施すことを意味する）に施した、 $h(IV), h^2(IV), h^3(IV), \dots, h^N(IV)$ なる値をそれぞれ対応させることとし、

各参加者 J は、前記 $1, 2, \dots, N$ の指標値に対し、 P_1, P_2, \dots, P_N なる値がその大小順に対応付けられている換算テーブルを参照して登録したい値と対応する指標値 i_J を求めて参加者端末装置により $(h^{N+1}(IV_J), g(h^{i_J}(IV_J)))$ なる一対の値を作成して中央装置へ送って意中の指標値 i_J を間接的に登録し、

中央装置は全ての参加者からの登録値を受信した後、

指標値 N , $N-1$, $N-2$, ...に登録した参加者 J がいるかどうかを、指標値の大きい順に各指標値ごとに全参加者端末装置に該当指標値 m の問合せ情報を送って尋ね、

参加者端末装置は受信した問合せ情報に対し該当しないときは、聞かれた指標値 m に対して $h^m(I V_J)$ を生成して前記中央装置へ送信し、

前記中央装置は受信した $h^m(I V_J)$ が $h^{N+1}(I V_J)$ から連なることを確認し、

前記問合せに対し参加者 K の指標値 i_K が該当するときはその参加者端末装置は少なくとも $h^{i_K}(I V_K)$ を生成して前記中央装置へ送信し、

前記中央装置は受信した $h^{i_K}(I V_K)$ から $g(h^{i_K}(I V_K))$ を生成し、これが先に登録したものと対応することを確認して、その指標値 i_K にて前記換算テーブルを参照して値 P_{i_K} を求め、その参加者 K が登録値 P_{i_K} が登録中の最大値又は最小値であることを出力することを出力することとを特徴とする大小比較方法。

【請求項8】 前記変換テーブルは前記 $P_1, P_2, P_3, \dots, P_N$ には $P_1 < P_2 < P_3 < \dots < P_N$ なる大小関係があり、かつ上位桁以上の値のみを示し、

参加者 J が間接的に登録したい値が、

その上位桁の値と該当する指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J との和 $P_{i_J} + Q_J$ で表現されるとき、前記参加者端末装置で $(h^{N+1}(I V_J), g(h^{i_J}(I V_J)))$ に Q_J を加え、 $(h^{N+1}(I V_J), g(h^{i_J}(I V_J)), Q_J)$ を前記中央装置へ送って登録し、

前記中央装置は各指標値 $N, N-1, N-2, \dots$ ごとに、全参加者の Q_J における大きいものから順次前記問合せを行うことを特徴とする請求項7記載の大小比較方法。

【請求項9】 前記変換テーブルは前記 $P_1, P_2, P_3, \dots, P_N$ が $P_1 > P_2 > P_3 > \dots > P_N$ なる大小関係があり、かつ、上位桁以上の値のみを示し、

参加者 J が間接的に登録したい値が、その上位桁の値と該当する指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J との和 $P_{i_J} + Q_J$ で表現されるとき、前記参加者端末装置は $(h^{N+1}(I V_J), g(h^{i_J}(I V_J)), Q_J)$ を前記中央装置へ送

って登録し、

前記中央装置は各指標値 $N, N-1, N-2, \dots$ ごとに全参加者の Q_J における小さいものから順次前記問合せを行うことを特徴とする請求項 7 記載の大小比較方法。

【請求項 10】 $1, 2, 3; \dots, N$ の N 種の指標値に対応して、初期値 I V に一方向性関数 h を多重に施して、 $H_1 = h(I \ V) \parallel f_1, H_2 = h(H_1) \parallel f_2, H_3 = h(H_2) \parallel f_3, \dots, H_N = h(H_{N-1}) \parallel f_N$ なる対応値をそれぞれ対応させ、フラグ $f_1 \sim f_N$ は意中の指標値 i の時の f_i とそれ以外の時のフラグとを異なる値として区別し、 $x \parallel y$ は x に y を連結することを示し、

各参加者 J は前記 $1, 2, \dots, N$ の指標値に対し、 P_1, P_2, \dots, P_N なる値がその大小順に対応付けられている換算テーブルを参照して登録したい値と対応する指標値 i_J のフラグ f_{i_J} を用いて参加者端末装置により $h(H_N)$ なる値を生成して中央装置へ送って意中の指標値 i_J を間接的に登録し、

前記中央装置は全ての参加者からの登録値を受信した後、

指標値 $N, N-1, N-2, \dots$ に登録した参加者 J がいるかどうかを、指標値の大きい順に各指標値ごとに全参加者端末装置に該当指標値 m の問合せ情報を送って尋ね、

参加者端末装置は受信した問合せ情報に対し該当しないときは、聞かれた指標値 m に対して $H_m = h(H_{m-1}) \parallel f_m$ に相当する値を生成して前記中央装置へ送信し、

前記中央装置は受信した $H_m = h(H_{m-1}) \parallel f_m$ が $h(H_N)$ から連なることを確認し、

かつ f_m により意中の値でないことを確認し、

前記問合せに対し参加者 K の指標値 i_K が該当するときはその参加者端末装置は、 $H_{i_K} = h(H_{i_K-1}) \parallel f_{i_K}$ を前記中央装置へ送信し、

前記中央装置はその受信した $H_{i_K} = h(H_{i_K-1}) \parallel f_{i_K}$ と共に登録したものとから登録したものであることを確認し、その指標値 i_K にて前記換算テーブルを参照して値 P_{i_K} を求め、その参加者 K が登録値 P_{i_K} が登録中の最大値又は最小値であることを特徴とする大小比較方法。

【請求項 1 1】 前記変換テーブルは前記 $P_1, P_2, P_3, \dots, P_N$ が $P_1 < P_2 < P_3 < \dots < P_N$ なる大小関係があり、かつ上位桁以上の値のみを示し、

参加者 J が間接的に登録したい値が、その上位桁の値と該当する指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J との和 $P_{i_J} + Q_J$ で表現されるとき、前記参加者端末装置は $(h(H_{NJ}), Q_J)$ を、前記中央装置へ送って登録し、

前記中央装置は各指標値 $N, N-1, N-2, \dots$ ごとに、全参加者の Q_J における大きいものから順次前記問合せを行うことを特徴とする請求項 1 0 記載の大小比較方法。

【請求項 1 2】 前記変換テーブルは前記 $P_1, P_2, P_3, \dots, P_N$ が $P_1 > P_2 > P_3 > \dots > P_N$ なる大小関係があり、かつ上位桁以上の値のみを示し、

参加者 J が間接的に登録したい値が、その上位桁の値と該当する指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J との和 $P_{i_J} + Q_J$ で表現されるとき、前記参加者端末装置は $(h(H_{NJ}), Q_J)$ を前記中央装置へ送信して登録し、

前記中央装置は指標値 $N, N-1, N-2, \dots$ ごとに全参加者の Q_J における小さいものから順次前記問合せを行うことを特徴とする請求項 1 0 記載の大小比較方法。

【請求項 1 3】 中央装置に登録値を登録し、中央装置で複数の参加者からの登録値中の最大値又は最小値を決めてもらう参加者端末装置のコンピュータに

上位桁の指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J よりなる登録値を入力する処理と、

参加者の固有の初期値 IV_J に対して $N+1$ 回多重一方向性関数 h を施した値 $h^{N+1}(IV_J)$ (N は指標値の種類の数) を生成する処理と、

IV_J に対し i_J 回多重一方向性関数 h を施し、更に一方向性関数 g を施した値 $g(h^{i_J}(IV_J))$ を生成する処理と、

上記 $h^{N+1}(IV_J)$ と上記 $g(h^{i_J}(IV_J))$ と上記 Q_J を登録情報 A_J として中央装置へ送信する処理と、

中央装置からの指標値 k を登録したかの問合せを受信する処理と、

上記受信した k について $h^k(IV_1)$ を生成する処理と、

上記 $h^k(I V_1)$ を上記中央装置に送信する処理と
 を実行させるプログラムを記録した記録媒体。

【請求項 1 4】 中央装置に登録値を登録し、中央装置で複数の参加者からの登録値中の最大値又は最小値を決めてもらう参加者端末装置のコンピュータに

上位桁の指標値 i_J と対応する値 P_{i_J} と下位桁の値 Q_J よりなる登録値を入力する処理と、

参加者の固有の初期値 $I V_J$ に対し一方向性関数 h を多重に施して $H_1 = h(I V_J) \parallel f_1$, $H_2 = h(H_1) \parallel f_2$, $H_3 = h(H_2) \parallel f_3$, ..., $H_N = h(H_{N-1}) \parallel f_N$, $h(H_N)$ (N は指標値の種類の数、 $f_1 \sim f_N$ はフラグでその 1 つは f_{i_J} であり、これは他のフラグと異なる値) を生成する処理と、

上記 $h(H_N)$ と Q_J を登録情報 A_J として中央装置へ送信する処理と、

中央装置から指標値 m を登録したかの問合せを受信する処理と、

上記受信 m に対し、 $H_m = h(H_{m-1}) \parallel f_m$ を生成する処理と、

上記 $H_m = h(H_{m-1}) \parallel f_m$ を上記中央装置に送信する処理と
 を実行させるプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、例えば電子競争入札方法に適用され、複数人の意中の値を比較する際に、最大または最小の意中の値を持つ者の値は知らせるが、それ以外の者の値は秘密裏にできる大小比較装置・方法およびそのプログラム記録媒体に関するものである。

【0002】

【従来の技術】

例えば電子競争入札は図 9 に示す様に、参加者毎に設けられる入札装置 11_1 , 11_2 , ..., 11_M と、これらと例えばネットワークで接続され、全体を統合的に処理する開票装置 12 から構成され、各 $1, 2, 3, \dots, N$ の N 種の指標値に対応して、初期値 $I V$ に一方向性関数 h を多重に施し、つまり $I V$ に i 回の一方

向性関数を施す場合、 $h^i(IV)$ と表現し、これは $h(h(h(\dots h(IV)\dots)))$ と h を i 回施すことを意味する。これら $h(IV)$ 、 $h^2(IV)$ 、 $h^3(IV)$ 、 \dots 、 $h^N(IV)$ なる値をそれぞれ指標値 $1, 2, 3, \dots, N$ と対応させることとし、各参加者 J ($J=1, 2, \dots, M$)はその入札装置 11_J から $A_J=(h^{N+1}(IV_J), g(h^{i_J}(IV_J)))$ なる一対の値を生成して、開票装置 12 に送ることで、その参加者 J の意中の指標値 i_J を間接的に登録する。 $g(x)$ は x に一方方向性関数 g を施すことを表わす。開票装置 12 は全参加者からの登録を受信した後、カウンタ 13 を初期値 N から順次ダウンカウントし、そのカウンタ 13 の各値 k ($N, N-1, \dots, 1$)について登録した参加者 J がいるかどうかを、全参加者端末装置 $11_1, \dots, 11_M$ に順次 k を送信して尋ね、毎回、該当しないときは、聞かれた指標値 k に対して $h^k(IV_J)$ に相当する値 B_J を各参加者装置 11_J から開票装置 12 へ応答することで $h^{N+1}(IV_J)$ から連なることを示し、ある参加者 K の指標値 i_K が該当するときになって初めて、 $h^{i_K}(IV_K)$ が開票装置 12 に受信され、これがその登録されていた $g(h^{i_K}(IV_K))$ に対応することで、登録された指標値中の最大値を予め登録していた者であることを証明する。このようにして開票装置は登録指標の大小比較を行うことが提案されている（例えば、特願平11-205004号）。

【0003】

この装置では前記 $1, 2, 3, \dots, N$ の N 種の指標値にそれぞれ対応している $P_1, P_2, P_3, \dots, P_N$ なる値が $P_1 < P_2 < P_3 < \dots < P_N$ なる大小関係が成立している場合には対応できるが、 $P_1 > P_2 > P_3 > \dots > P_N$ なる大小関係が成立している場合にはそのままでは対応できなかった。

また、第2の問題として、比較対象の N 種の指標値が限定される場合、例えば、 $1 \sim 1$ 億までの数を区別したくても、 N が限定され、例えば、一万種しか無かった場合、便宜的に1万刻みに、1万、2万、 \dots 、9999万、1億という表現しかゆるされなかった。しかし、本当は1刻みで大小判定をしたかったが、このようなことは従来は実質的にはできなかった。

【0004】

【発明が解決しようとする課題】

この発明の目的は一種の大小判定の機能により、最大値検出と最小値検出の両方を同一の手法で実行できる大小比較方法を提供することにある。

この発明の他の場合は指標値の表現種類が限定される場合でも、任意の桁の範囲で大小判定をすることを可能にする比較方法を提供することにある。

【0005】

【課題を解決するための手段】

第一の課題は、内部的な指標値と外部的な対応値の対応付けを与える手段を設けることにより、同じ演算機能を最大または最小の複数の目的で使えることにする。

第二の課題は、前記外部的な対応値において、ある桁以上は大小判定にとって重要なので秘密裏に扱うが、その桁未満は公開しても、実質的な重要性が低いので、下の桁の大小により比較の順番をつけて公表する手段を設け、任意の桁の範囲での大小比較を可能とする。

【0006】

【発明の実施の形態】

以下図面を用いてこの発明の実施例について詳しく説明する。

第一の実施例

電子競争入札を例とした場合で、図1に示すように複数の参加者 J ($J = 1, 2, \dots, M$)の入札装置 11_J と開票装置12とで構成され、これらは通信手段で互いに接続することが可能である。入札装置 11_J は1つしか示していないが複数存在する。この実施例では内部的な指標値 $1, 2, \dots, N$ と外部的な対応値 $10, 15, \dots, 3000$ との対応付けを示す換算テーブル21が入札装置 11_J 、開票装置12にそれぞれ設けられている。

【0007】

$1, 2, 3, \dots, N$ の N 種の指標値 k に対応して、初期値 IV に一方向性関数 h を多重（例えば、 IV に i 回の一方向性関数を施す場合、 $h^i(IV)$ と表現することにする。但し、意味は h と i 回施す $h(h(h(\dots h(IV)\dots)))$ と同様である）に施した、 $h(IV)$ 、 $h^2(IV)$ 、 $h^3(IV)$ 、 \dots 、 $h^N(IV)$ なる値をそれぞれ対応させることとし、各参加者 J は意中の指標値 k が i

J の場合入札装置 11_J により $(h^{N+1}(IV_J), g(h^i_J(IV_J)))$ なる一対の値を生成し、これら開票装置 12 へ送信することにより意中の指標値 i_J を間接的に登録する。

【0008】

全参加者からの登録が終了した後、開票装置 12 はカウンタ 13 に最大指標値 N を初期値として設定し、このカウンタ 13 の値 $k=N$ を登録した参加者 J がいるかどうかを全参加者の入札装置 11_J に $k=N$ を送って尋ねる。入札装置 11_J はその問合せに該当しないときは、聞かれた指標値 k に対して $h^k(IV_J)$ を生成して開票装置 12 へ送って回答する。開票装置 12 はその受信した $h^k(IV_J)$ が先に登録した $h^{N+1}(IV_J)$ から連なることを知る。全参加者から回答が該当しない時はカウンタ 13 を 1 ダウンカウントして $k=N-1$ として同様の問合せを行う。以下同様のことを行う。ある参加者の指標値 i_K が該当するときになって初めてその入札装置 11_K から受信した $h^{i_K}(IV_K)$ に対し $g(h^{i_K}(IV_K))$ を求め、これが登録されていた $g(h^{i_K}(IV_K))$ と一致することで、指標における最大値を予め登録していた者であることを証明する。

【0009】

この場合は換算テーブル 21 において $1, 2, 3, \dots, N$ の N 種の指標値に対応した外部的対応値 $P_1, P_2, P_3, \dots, P_N$ なる値は $P_1 < P_2 < P_3 < \dots < P_N$ なる大小関係が成立するように対応付けられてある。従って前述したように開票装置 12 で登録されている指標値中の最大値が検出されるから、その最大値の登録指標値 i_k と対応する外部的対応値 P_{i_k} は各参加者が意中の登録した値中の最大値を示すことになる。

【0010】

なお開票装置 12 は全参加者が登録後にその登録値 $(h^{N+1}(IV_J), g(h^{i_J}(IV_J)))$ を出力公開し、また求めた最大登録指標値 i_J と、その登録参加者 J を出力表示する。

第二の実施例

この実施例は図 2 に示す様に、図 1 に示した構成とほぼ同様であり、その指標値の開票装置 12 への登録、開票装置 12 における登録最大指標値とその参加者

を求める処理も同様である。

【 0 0 1 1 】

第一の実施例と異なる点は、換算テーブル 2 1 の内容である。つまりこの場合の換算テーブル 2 1 において 1, 2, 3, ..., N の N 種の指標値に対応した外部対応値 $P_1, P_2, P_3, \dots, P_N$ なる値は $P_1 > P_2 > P_3 > \dots > P_N$ なる大小関係が成立するように対応付けられてある。図 2 の例では指標値 1 は 3 0 0 0、2 は 2 9 1 3、3 は 2 9 0 0 と指標値が大きくなるに従って外部対応値 P_k は小さくなる。従って求められた登録指標値中の最大値 i_k と対応する外部対応値 P_{i_k} は全参加者が意中の登録した値中の最小値を示すことになる。

【 0 0 1 2 】

このようにこの発明では換算テーブル 2 1 の指標値と対応値との大小関係を逆にすることにより、同一構成、同一処理手順で最大値を求めることも最小値を求めることの何れにも変更できる。

第三の実施例

第三の実施例は図 3 に示す様に、入札装置 1 1_J、開票装置 1 2、共通の換算テーブル 2 1 を備えることは第一の実施例と同一である。

【 0 0 1 3 】

ただ処理が以下のように異なる。1, 2, 3, ..., N の N 種の指標値に対応して、初期値 IV に一方向性関数 h を多重に施して、 $H_1 = h(IV) \parallel f_1$, $H_2 = h(H_1) \parallel f_2$, $H_3 = h(H_2) \parallel f_3$, ..., $H_N = h(H_{N-1}) \parallel f_N$ なる値をそれぞれ対応させる。フラグ $f_1 \sim f_N$ は意中の指標値 i の時の f_i とそれ以外の時のフラグと異なる値として区別できるものとする。例えば入札指標値のフラグ f_i は 1 とし、非入札指標値 p のフラグ f_p は 0 とする。 $x \parallel y$ は x に y を連結することを示すとき、参加者 J は入札装置 1 1_J で初期値 IV_J に対し、前記多重に一方向性関数 h を施すがその際、連結するフラグ f を、入札したい指標値に対しては例えば 1 とし、その他の指標値と対応するフラグは 0 として $h(H_N)$ を生成して意中の指標値 i_J を間接的に登録する。

【 0 0 1 4 】

全参加者の登録が終わった後、開票装置 1 2 は指標値 $N, N-1, N-2, \dots$ の

それぞれごとに登録した参加者 J がいるかどうかを登録指標値を全参加者の入札装置に送って尋ね、入札装置は該当しないときは、聞かれた指標値 k に対して $H_k = h(H_{k-1}) \parallel f_k$ に相当する値を開票装置 12 へ返送することで $h(H_N)$ から連なることを示すとともに f_k により意中の値でないことを示し、ある参加者 K の指標値 i_K が該当するときに初めて、その入札装置 11_K から送られた $H_{i_K} = h(H_{i_K-1}) \parallel f_{i_K}$ が登録してあるものと一致し、その f_{i_K} が意中の指標値にあることが求まる。この指標値が登録中の最大値であり、その回答がその指標値を予め登録していた者であることを証明することができる。なお、この明細書においては例えば $i_K - 1$ を添字として用いる時は $i_K - 1$ と表し、他の添字も同様である。

【0015】

この場合換算テーブル 21 の 1, 2, 3, ..., N の N 種の指標値に対応する、 $P_1, P_2, P_3, \dots, P_N$ なる値は $P_1 < P_2 < P_3 < \dots < P_N$ なる大小関係が成立するようにされてある。よって求めた登録最大値の指標値 i_K は最大入札値 P_{i_K} となる。

第四の実施例

図 4 に示す様に、図 3 に示した場合と同様の構成、同様の処理を行うが、換算テーブル 21 は 1, 2, 3, ..., N の N 種の指標値に対応する、 $P_1, P_2, P_3, \dots, P_N$ なる値が $P_1 > P_2 > P_3 > \dots > P_N$ なる大小関係が成立しているようにされてある。従って、求めた登録最大値の指標値 i_K は最小入札値 P_{i_K} となる。

第五の実施例

図 5 に示す様に、図 1 に示した構成と同様であり、処理もほぼ同様であるが、換算テーブル 21 において指標値 1, 2, 3, ..., N と対応する値 $P_1, P_2, P_3, \dots, P_N$ は $P_1 < P_2 < P_3 < \dots < P_N$ なる大小関係が成立していることも同様であるが、これら $P_1, P_2, P_3, \dots, P_N$ はある桁以上の値、つまり上位桁の値のみを示し、図では指標値 1 は 1000、2 は 2000、3 は 3000... と 4 桁以上の値である。

【0016】

参加者 J が入札したい値を、その上位桁（前記ある桁）以上の値と該当する指

標値 i_J と対応する値 P_{i_J} と下位桁の値、つまり前記ある桁未満の値 Q_J との和 $P_{i_J} + Q_J$ で表現し、図 1 で生成した $(h^{N+1}(IV_J), g(h^{i_J}(IV_J)))$ に Q_J を加え、 $(h^{N+1}(IV_J), g(h^{i_J}(IV_J)), Q_J)$ を開票装置 12 へ送って登録する。

開票装置 12 は各指標値についてその大きい順に参加者の入札装置に問合せを行うが、各指標値ごとに、全参加者の Q_J における大きいものから（降順に）順次尋ねる。聞いた指標値に対し、登録した参加者が求めれば、その問合せ指標値についてまだ問合せをしていない参加者がいても、以後の問合せを中止する。なお問合せ k に対し、 $h^k(IV_J)$ を回答することは図 1 の場合と同様である。

【0017】

以上のようにして指標値の種類が少なく、複数人が例え同じ対応値 P_i または指標値 i を指定したとしても、ある桁以下の Q_J 値の大小により互いに区別し、真に最大値となる参加者および値を示すことができる。

第六の実施例

図 6 に示す様に、図 5 と同様な構成であるが、換算テーブル 21 において指標値 1, 2, 3, ..., N と対応する値 $P_1, P_2, P_3, \dots, P_N$ が $P_1 > P_2 > P_3 > \dots > P_N$ なる大小関係とされており、かつある桁以上の値のみを示す価である。参加者 J が間接的に登録したい値を、ある桁以上の値の指標値 i_J と対応する値 P_{i_J} と前記桁未満の値 Q_J との和 $P_{i_J} + Q_J$ で表現し、図 5 の場合と同様に $(h^{N+1}(IV_J), g(h^{i_J}(IV_J)), Q_J)$ を開票装置 12 へ送り登録する。

【0018】

開票装置 12 は各指標値ごとの登録をしているかの問合せを大きい順、つまり N から $N-1, N-2, \dots$ と行うが、その各指標値ごとに全参加者の Q_J における小さいものから（昇順に）順次尋ね、参加者の回答が登録したものとなる場合にその指標値についての問合せが済んでなくても問合せを中止する。

以上のようにして指標値の種類が少なく、複数人が例え同じ対応値 P_i または指標値 i を指定したとしても、ある桁以下の Q_J 値の大小により互いに区別し、真に最小値となる参加者および値を示すことができる。

第七の実施例

図 7 に示す様に、図 3 に示した構成及び処理とほぼ同様であるが換算テーブル 2 1 は図 5 に示したものと同様なものが用いられ、従って参加者 J が間接的に登録したい値を、図 5 で説明したように $P_{iJ} + Q_J$ と表現し、入札装置から $H_{(N+1)J} = h(H_{NJ})$ に Q_J を加え、 $(H_{(N+1)J}, Q_J)$ を開票装置 1 2 へ送信して登録する。

【 0 0 1 9 】

開票装置 1 2 での各指標値についての登録したかの問合せは図 5 の実施例と同様に指標値 N から、N - 1, N - 2, ... に対応する P_{iJ} を登録した参加者 J がいるかどうかを、各指標値ごとに全参加者の Q_J における大きいものから（降順に）順次尋ねる。

問合せ m に対し $H_m = h(H_{m-1}) \parallel f_m$ を応答することは図 3 の場合と同様である。

【 0 0 2 0 】

このようにして指標値の種類が少なく、複数人が例え同じ対応値 P_i または指標値 i を指定したとしても、ある桁以下の Q 値の大小により互いに区別し、真に最大値となる参加者および値を示すことができる。

第八の実施例

図 8 に示す様に、図 4 に示した構成及び処理とほぼ同様であるが換算テーブル 2 1 は図 6 に示したものが用いられ、入札値の登録は図 7 の場合と同様に参加者 J が間接的に登録したい値を $P_{iJ} + Q_J$ で表現し、 $H_{(N+1)J} = h(H_{NJ})$ に Q_J を加え、 $(H_{(N+1)J}, Q_J)$ を送信登録する。

【 0 0 2 1 】

開票装置 1 2 で各指標値ごとにその大きい順から対応する P_{iJ} を登録した参加者 J がいるかどうかを、全参加者の Q_J における小さいものから（昇順に）順次尋ねる。

このようにして指標値の種類が少なく、複数人 J が例え同じ対応値 P_{iJ} または指標値 i_J を指定したとしても、ある桁以下の Q_J 値の大小により互いに区別し、真に最小値となる参加者および値を示すことができる。上述ではこの発明を電子競争入札方法に適用したが、その他の場合でも複数の参加者が中央装置にある値

を登録し、その最大値又は最小値を求め、それ以外のものを明かさずに済む場合に適用できる。また上述の各装置はコンピュータによりプログラムを解読実行させて機能させることもできる。

【 0 0 2 2 】

【発明の効果】

上記各種実施例に示す様に、第一～第四の実施例によれば、N種類の値に関して大小比較する装置により、最大値選定または最小値選定を、選定されないものの価を明かさずに実行できる。また、第五～第八の実施例によれば、値がN種以上の表現範囲がある比較において、中央装置によって比較する部分を上位桁に限定し、下位の桁は予め明かし、大小比較時においても順番付けをすることにより、N種類の値に関して大小比較する装置により、最大値選定または最小値選定を選定されないものの価を明かさずに実行できる。

【図面の簡単な説明】

【図 1】

第一の実施例を示す図。

【図 2】

第二の実施例を示す図。

【図 3】

第三の実施例を示す図。

【図 4】

第四の実施例を示す図。

【図 5】

第五の実施例を示す図。

【図 6】

第六の実施例を示す図。

【図 7】

第七の実施例を示す図。

【図 8】

第八の実施例を示す図。

【図 9】

提案されている電子競争入札装置を示す図。

【書類名】 図面

【図 1】

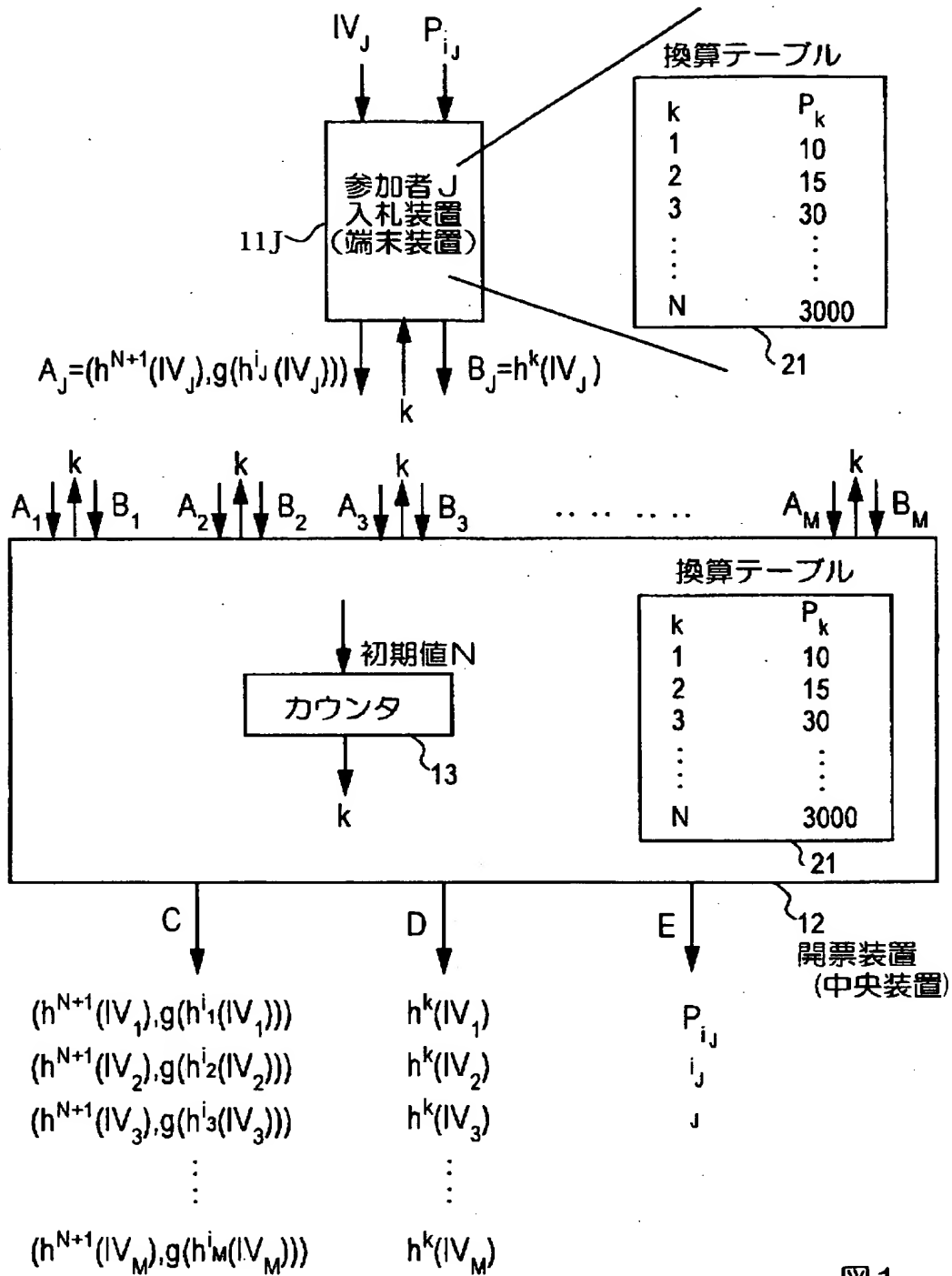


図 1

【図 2】

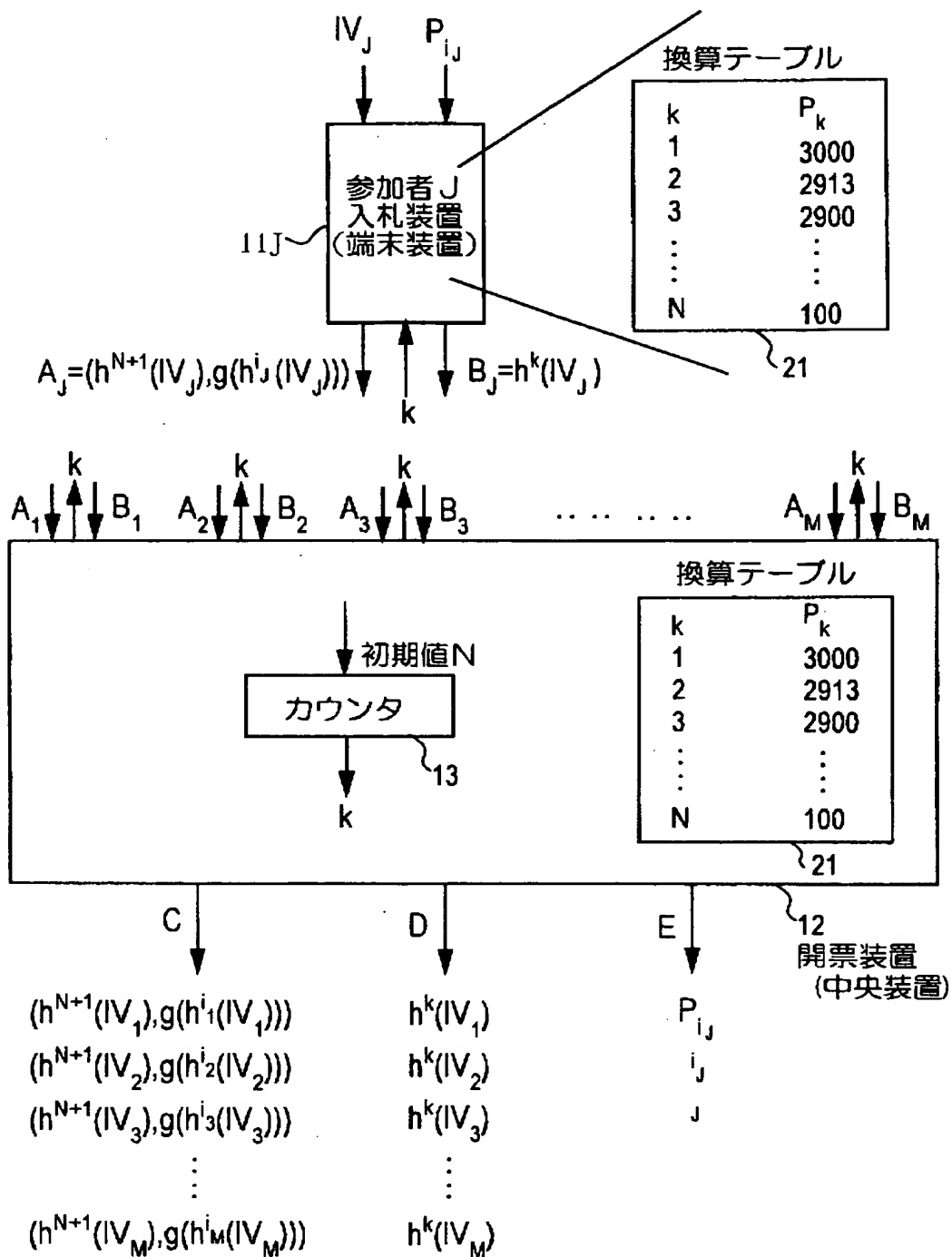


図2

【図 3】

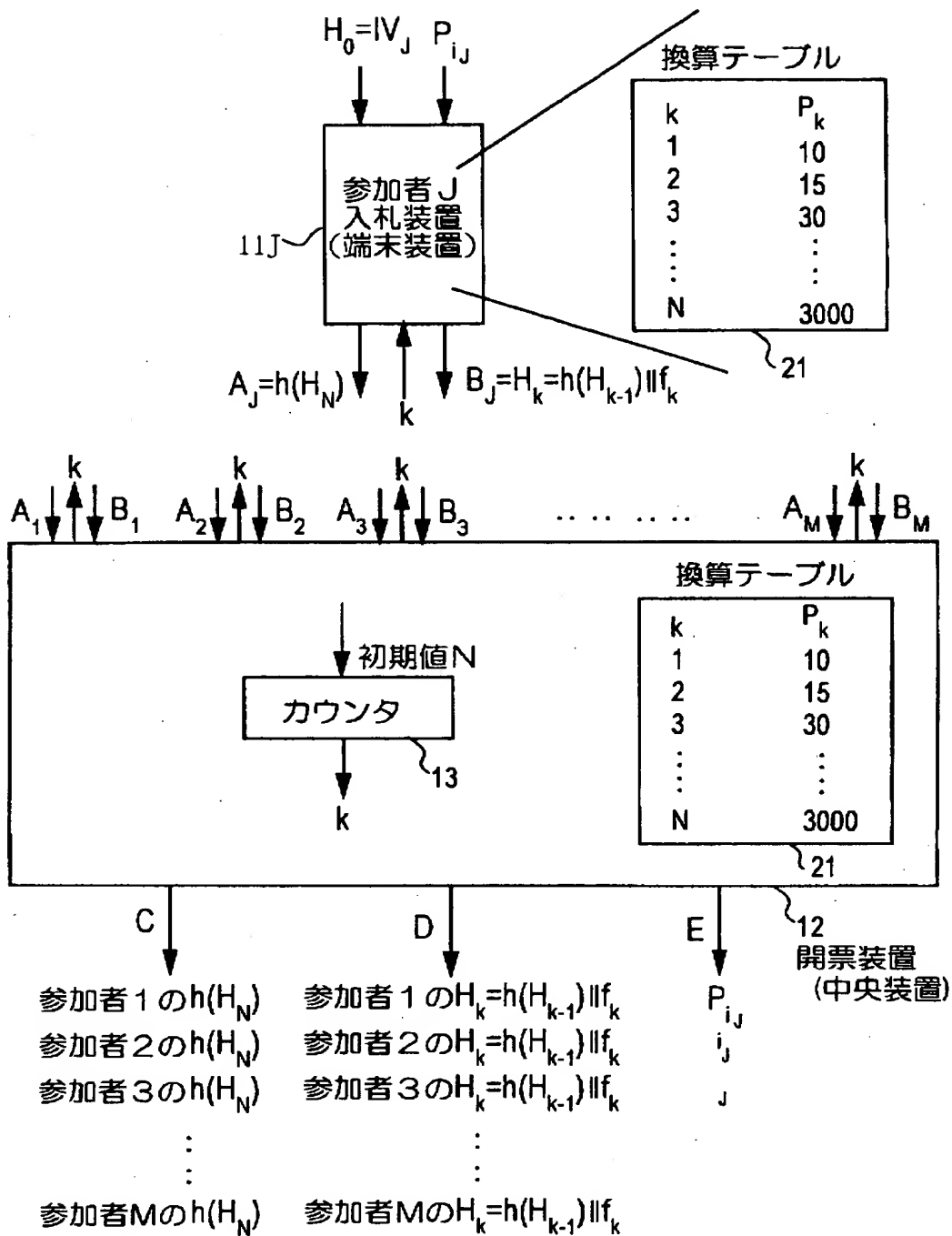


図3

【図 4】

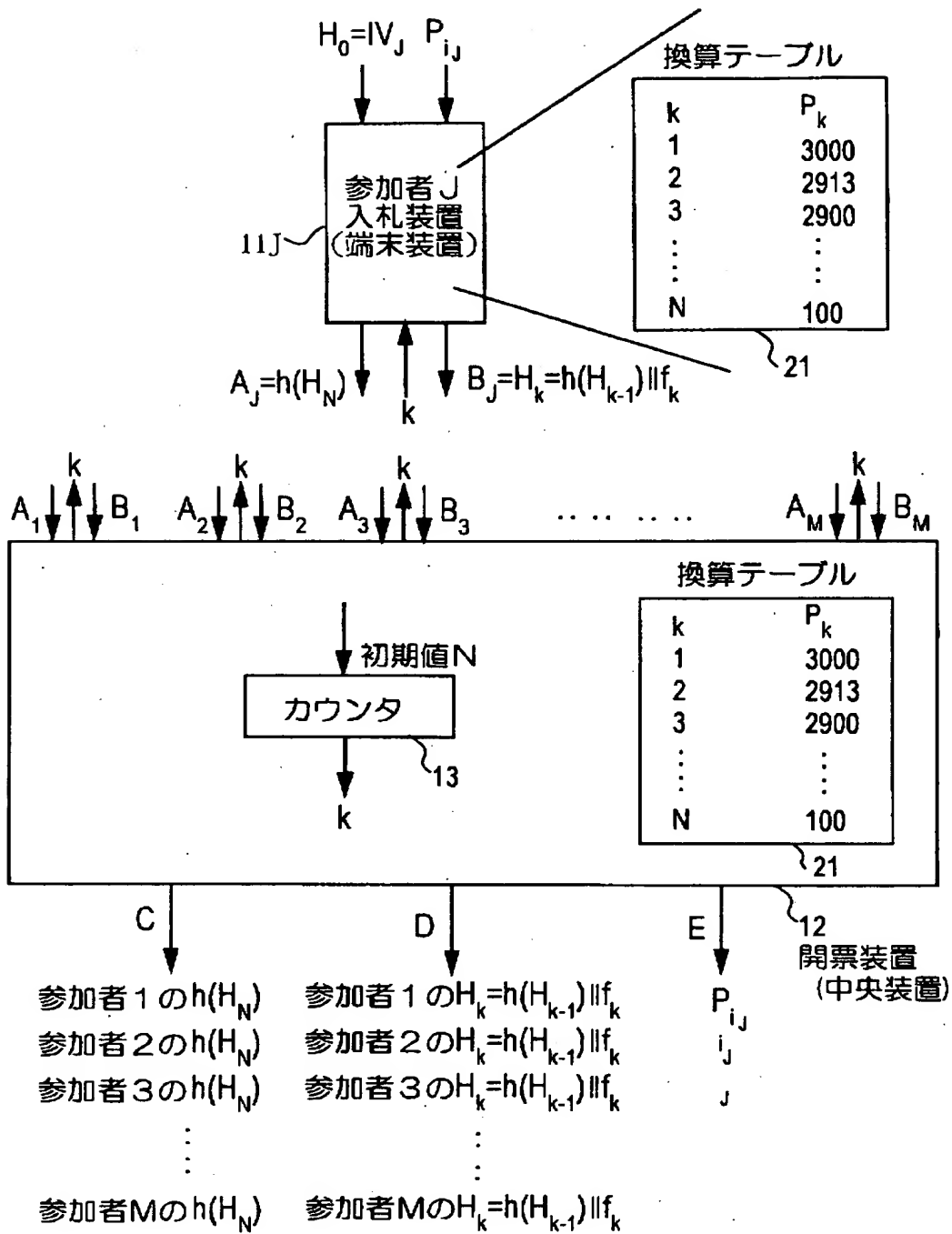


図 4

【図 5】

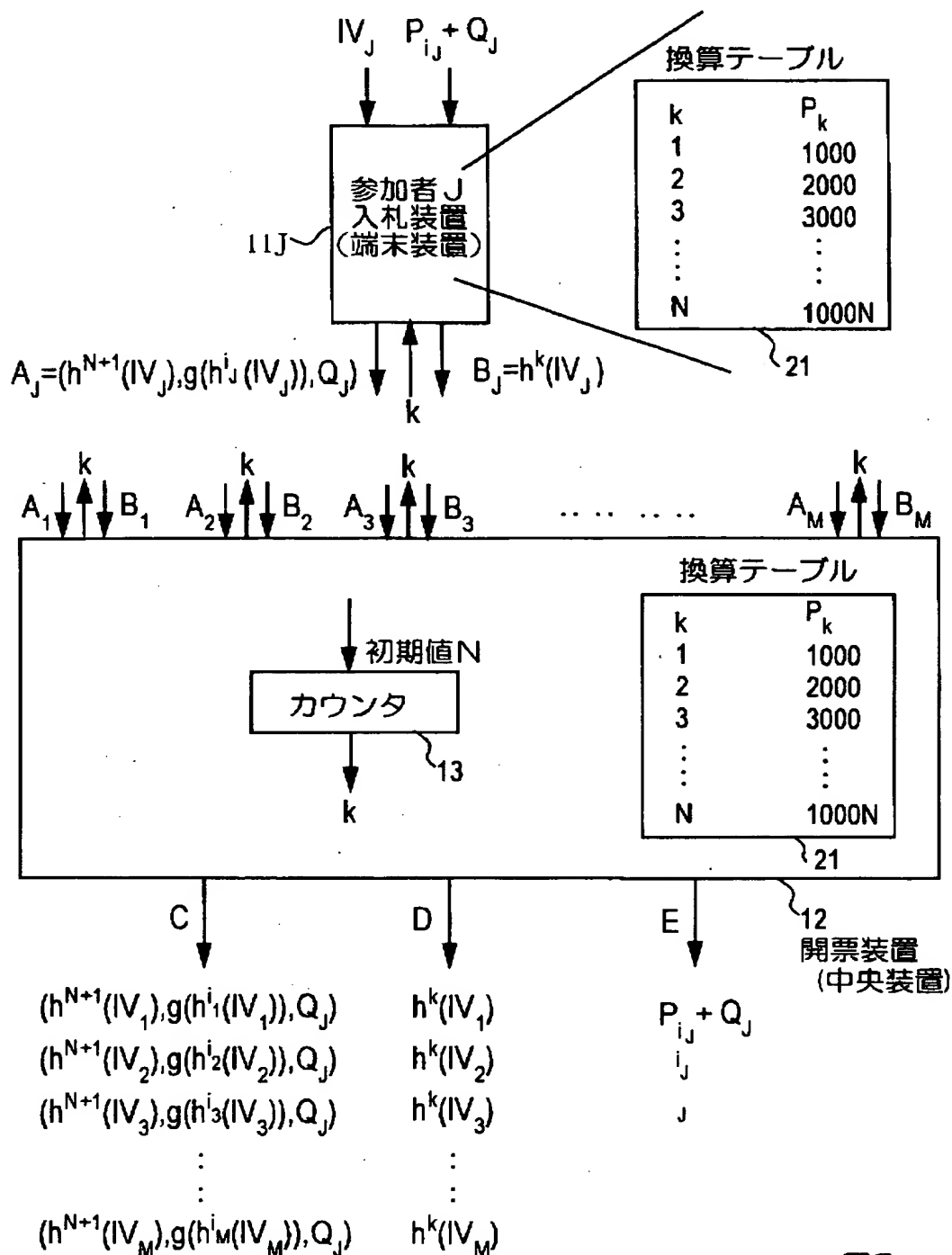


図5

【図 6】

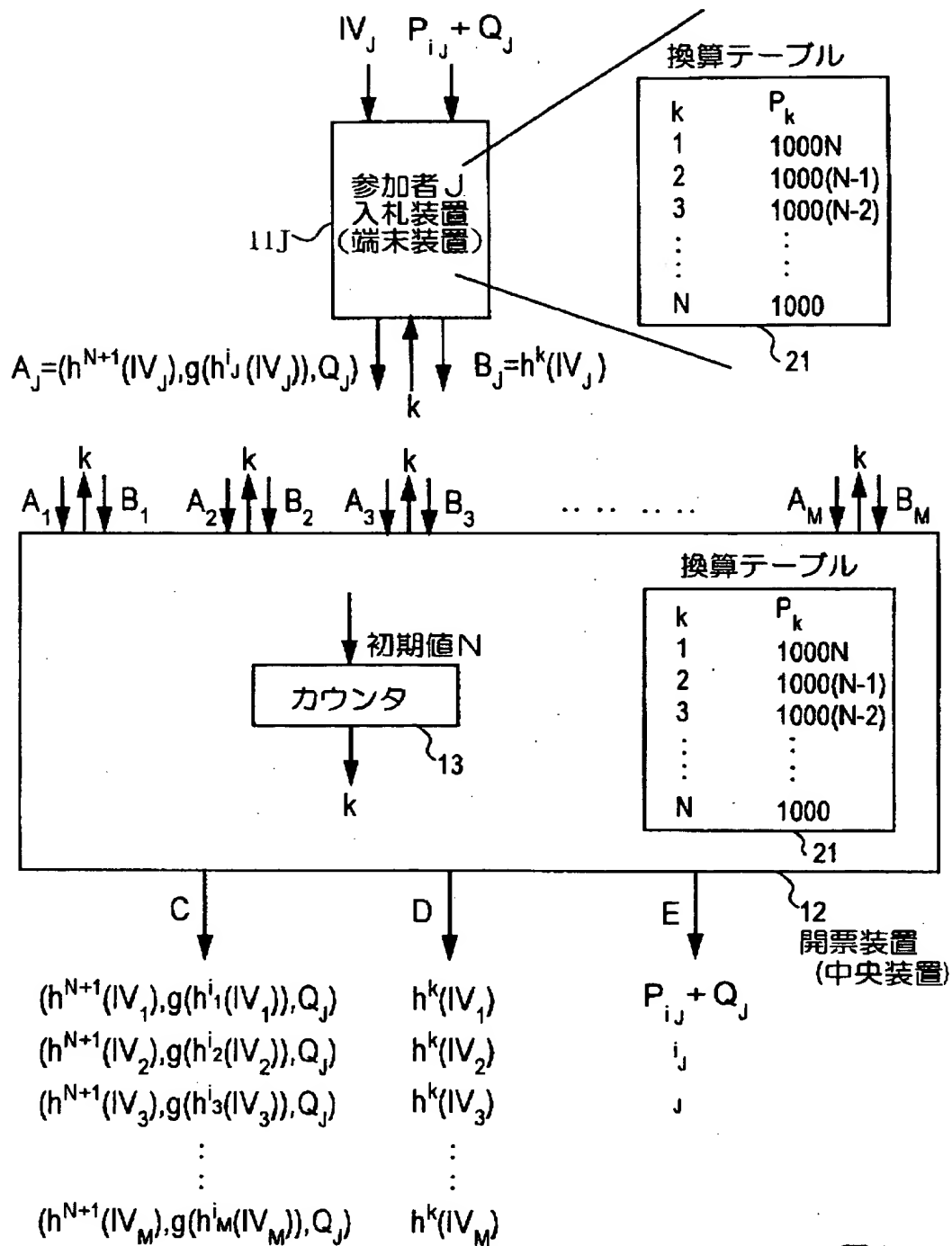


図6

【図 7】

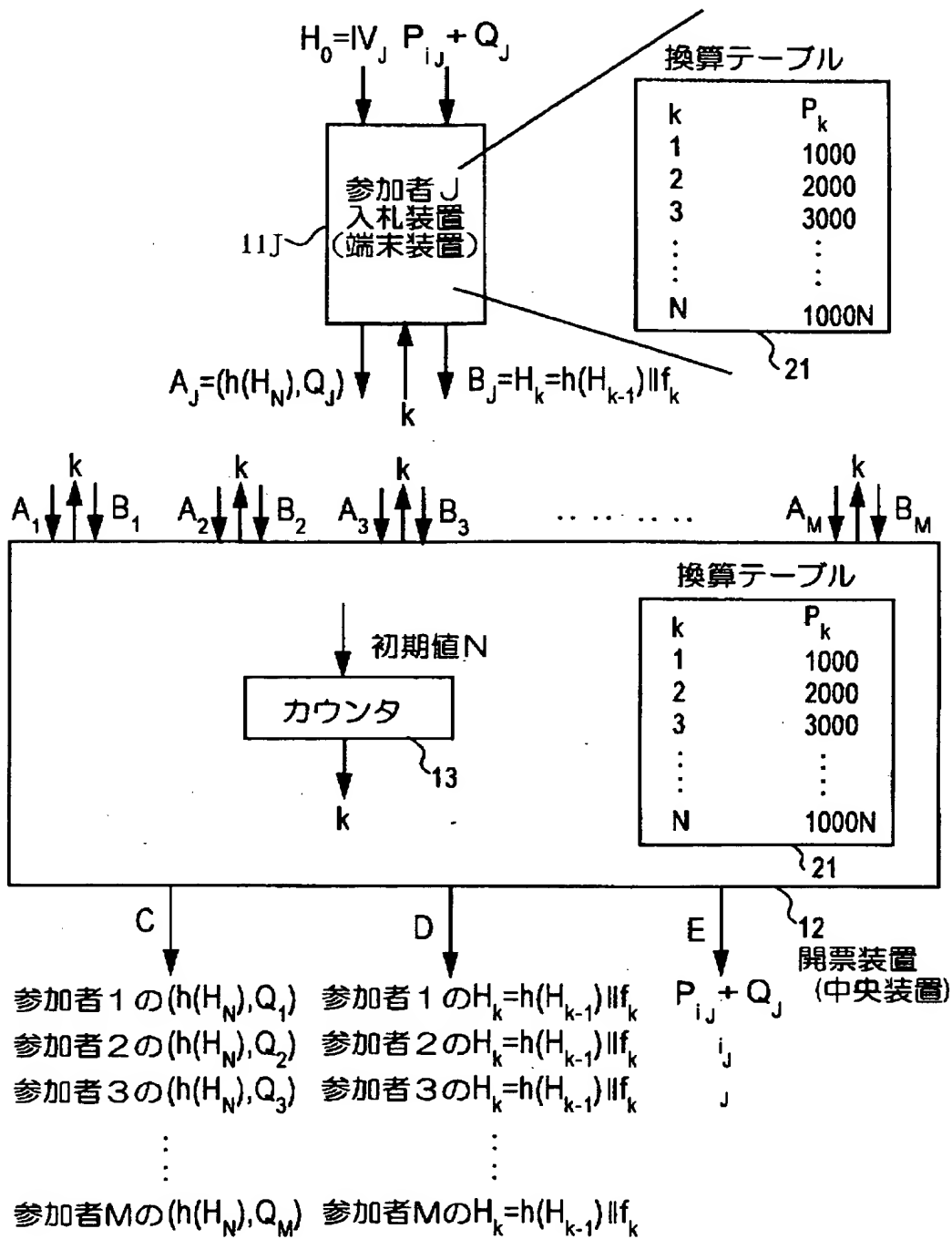


図7

【図 8】

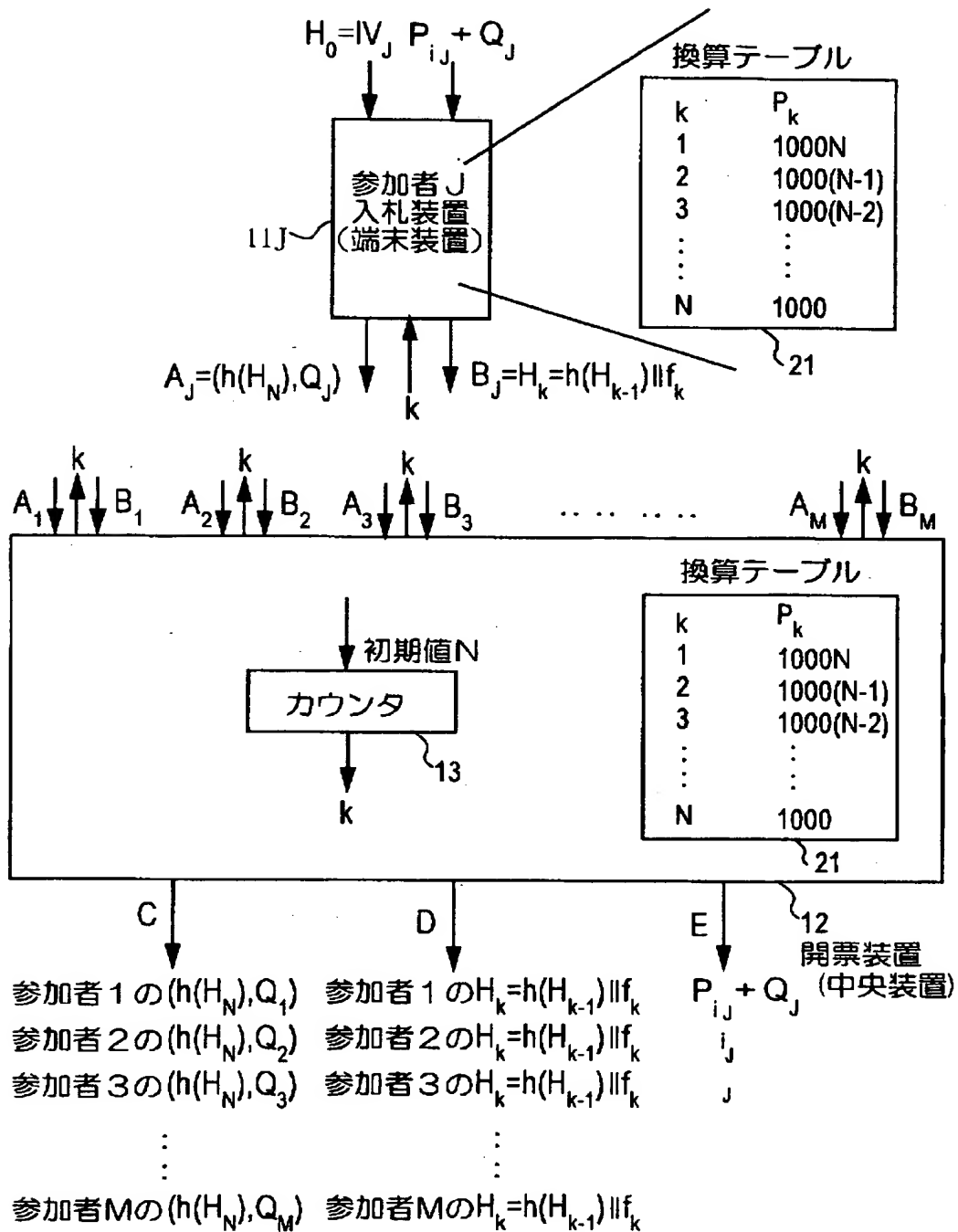


図8

【図 9】

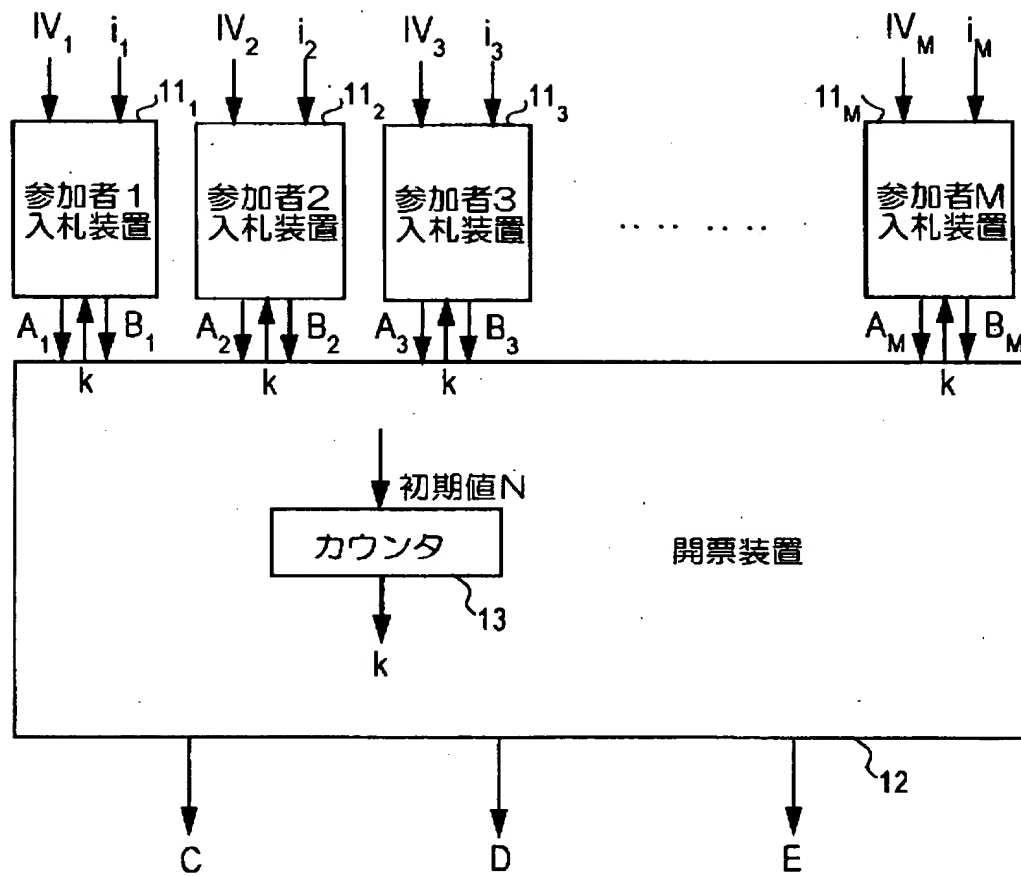


図9

【書類名】 要約書

【要約】

【課題】 例えば電子競争入札において同一構成、同一処理で最大値又は最小値を求めることを可能とする。

【解決手段】 指標値 (k) $1, 2, \dots, N$ と対応する値 (P_k) P_1, P_2, \dots, P_N との換算テーブル 2 1 を入札装置、開票装置 1 2 に設け、参加者 J は入札値 P_{iJ} と対応した指標値 i_J を求め、 J の初期値 IV_J を初期として多重ハッシュした値 $h^{N+1}(IV_J)$ と $g(h^{i_J}(IV_J))$ を求め、開票装置 1 2 へ送り、全参加者が登録し終ると、装置 1 2 は N から順に登録したかの問合せを全参加者へ送り、指標値 m に対して、各参加者は $h^m(IV_J)$ を返送し、登録してある $g(h^{i_J}(IV_J))$ と一致したものを受信すると、その時の m を登録中の最高指標値とし、その登録した値を明らかにする、テーブル 2 1 が指標 $1, \dots, N$ に対し $P_1 < \dots < P_N$ であれば入札最大値が求まり、テーブル 2 1 が $1, \dots, N$ に対し $P_1 > \dots > P_N$ であれば入札最小値が求まる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日 1999年 7月15日
[変更理由] 住所変更
住 所 東京都千代田区大手町二丁目3番1号
氏 名 日本電信電話株式会社